



SN 09/518,664

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Cameron Mashayekhi	Examiner:	Matthew Heneghan
Serial No.:	09/518,664	Group Art Unit:	2134
Filed:	March 3, 2000	Docket:	1565.027US1
Title:	APPARATUS AND METHOD FOR AUTOMATICALLY AUTHENTICATING A NETWORK CLIENT		

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

The Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request. This request is being filed with a Notice of Appeal. The review is requested for the reasons stated below:

§103 Rejection of the Claims

Claims 1-11, 13, 15, 17-18 and 20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Khan et al. (U.S. 6,401,206) in view of Mashayekhi (U.S. 5,818,936) and further in view of Menezes ("Handbook of Applied Cryptography"). It is of course fundamental that in order to sustain an obviousness rejection that each and every step or element in the rejected claims must be taught or suggested in the proposed combination of references. Moreover, there must exist some motivation by one of ordinary skill in the art to combine the references in the manner proposed by the Examiner.

Applicant continues to respectfully disagree with the Examiner with respect to the interpretation of the Khan reference and modification and combination with the Menezes. Applicant understands that a term in the claims must be given its broadest possible interpretation as asserted by the Examiner. However, Applicant disagrees in that a term cannot be given such a broad interpretation that it actually conflicts with how that term is understood in the art and defined in the art absent some contrary lexicographer using in the original filed specification. Here, there is no such contrary usage in the Applicant's original filed specification. Consequently, the phrase "session key" cannot be distorted in an attempt to make it so broad that it actually flies in the face of how that phrase is used in the industry and commonly understood in

the industry.

The Menezes reference declares what a session key is and how it is understood and that definition and usage is exactly what the industry recognizes and what the Applicant has been trying to convey. Specifically, Menezes states that a session key is “one whose use is restricted to a short time period . . .” Menezes, referencing the section entitled “Motivation for Use of Session Keys.” This section goes on to state that the session key is used to “limit exposure” of the key and “avoid long term storage” of the key. Clearly, Menezes comports with the definition and understanding of “session key” as that term is understood in the industry.

Again, by definition a “session key” is a key that is “frequently changed” and a “different session key may be used for each message” of a transaction. See, <https://whatis.techtarget.com/keyphrase/sessionkey>. Applicant has personally traversed the above link that is associated with “Whatis.com” and said link does exist and does work for the Applicant and did work at the time that Applicant submitted the prior response to the Examiner. As an alternative, the Examiner is invited to visit Wikipedia at http://en.wikipedia.org/wiki/Main_Page and search on “session key.” At this site, the definition specifically states that session keys are not associated with users and solve problems that are different from “public keys;” stating public keys are too slow and impractical for long messages and that session keys addresses this particular problem. The beginning definition also states that session keys are used to encrypt messages; rather than users as is the case with public keys. Applicant does not believe there is any ambiguity in the art as to what a session key is and as to whether there is a clear distinction between a public key and session key because the two types of keys are different and address different problems in cryptography. Therefore, Applicant respectfully continues to disagree with the manner in which the Examiner appears to have couched or transformed a session key into a public key for purposes of finding the teachings in the Khan reference to render Applicant’s claims obvious.

Juxtapose the way the industry recognizes a session key and understands it and with the way that Menezes agrees with that interpretation with the Kahn reference. The Khan reference only discusses and uses three types of keys a “private key,” a “public key” and a “symmetric key.” There is no dispute with the Examiner on record in that the “private key” is not a “session key,” since clearly a private key is known to just one party and is not communicated beyond that party and the private key is not common and is not usable beyond a party to which it relates. The

dispute arises with the “public key.”

With respect to Khan’s “public key,” the digital identity in Khan is not intended to be temporary. Khan specifically states the identity is permanent. See, Khan col. 8 lines 20-29 where it is specifically stated that the digital identity is “generated once in its lifecycle.” Column 11 in Khan lines 65 and continuing to column 12 line 32 emphasizes that digital identity is intended to be permanent and not temporary. Applicant’s claims state that “use” expires when the “session expires.” Clearly, this is not permanent.

Moreover, Applicants respectfully continue to assert that Khan cannot be used in connection with Menezes because there would have been no motivation by one of ordinary skill in the art to do so. This is so because Menezes uses a session key that creates temporary identities and Khan specifically calls for and emphasizes the importance of permanency for identities. One of ordinary skill in the art would not have read Khan and Menezes and been motivated to combine the two because Khan teaches away from Menezes and Menezes teaches away from Khan. The Examiner asserts that because someone can modify their own digital identity as suggested in Khan at column 8 lines 37-46 that this is sufficient to demonstrate a motivation because it is suggested that the identities may be modified and thus be temporary. Applicant respectfully disagrees with this interpretation because the public key is not changed for the identity in Khan when this occurs. The prior paragraph at column 8 lines 30-36 provides the context within which the statements at column 8 lines 37-46 are made and there it is clear that the symmetric key is changed for the identity and not the public key which remains permanent and stable.

The core issue in the rejection appears to be whether a session key is temporary and frequently changed. The Examiner continues to maintain that this interpretation has no basis in the art. Applicant respectfully disagrees and has supplied two references above for art definitions and reserves the right to find numerous others on appeal. Another issue is whether the Khan reference would even support a session key. Applicant respectfully asserts that to do so would actually run contrary to the core teachings of Khan and as such it is has been held when there is evidence of this there is no motivation by one of ordinary skill in the art to combine teachings. Thus, the combined references lack each and every teaching of the claims of record and the combination of references is improper. As such, Applicant respectfully request that the

rejections of record be withdrawn and the claims allowed.

Claims 12, 14, 16 and 19 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Khan et al. in view of Mashayekhi and further in view of Menezes as applied to claims 9 and 15 above, and further in view of Spies et al. (U.S. 5,869,565). Claims 12 and 14 are dependent from independent claim 9, claims 16 and 19 are dependent from independent claim 15; therefore, for the remarks supplied above with respect to independent claims 9 and 15, the rejections of claims 12, 14, 16, and 19 should be withdrawn. Applicant respectfully request an indication of the same.

CONCLUSION

The Applicant respectfully submits that all of the pending claims are in condition for allowance, and such action is earnestly solicited. The Examiner is invited to telephone the below-signed attorney at (513) 942-0224 to discuss any questions which may remain with respect to the present application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

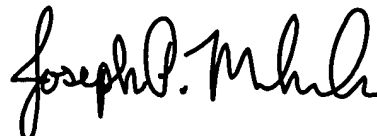
CAMERON MASHAYEKHI

By his Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
(513) 942-0224

Date July 24, 2006

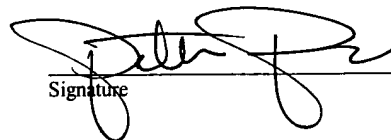
By



Joseph P. Mehrle
Reg. No. 45,535

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this 24 day of July 2006.

Peter Reibon
Name


Signature